

Image of Client Logo

Penetration Testing Report

All Ports Tours Cruise Line (APT)

Prepared by: Our Company Name

September 17, 2025

CONFIDENTIAL

Table of Contents

1.0 Report Overview 4

 1.1 Confidentiality 4

 1.2 Legal Disclaimer 4

 1.3 Contact Information 4

2.0 Executive Summary 5

 2.1 Assessment Overview 5

 2.1.1 Phases of Penetration Testing 5

 2.2 Scoping and Time Limitations 6

 2.3 Testing Summary 6

 2.4 Tester Notes & Recommendations 6

3.0 Assessment Components 7

 3.1 Open-Source Intelligence 7

 3.2 External Penetration Test 7

 3.3 Internal Penetration Test 7

4.0 Scope 8

 4.1 Scope Exclusions 8

 4.2 Client Allowances 8

 4.3 Network Topology 8

5.0 Compliance Summary 9

 5.1 Compliance1 9

 5.2 Compliance2 9

6.0 Technical Finding Summary 10

7.0 Technical Findings	11
7.1 Critical Risk Findings	11
7.1.1 [Finding Name]	11
7.2 High Risk Findings	11
7.2.1 [Finding Name]	11
7.3 Medium Risk Findings	12
7.3.1 [Finding Name]	12
7.4 Low Risk Findings	13
7.4.1 [Finding Name]	13
7.5 Informational Risk Findings	14
7.5.1 [Finding Name]	14
Example: Payment Card Industry Data Security Standard (PCI DSS)	15
Appendix A: Social Engineering	16
Methodology	16
Results	16
Appendix B: Methodologies	17
Testing Frameworks	17
Diagrams	17
Appendix C: Attack Paths	19
Visualizations	19
Appendix D: Risk Assessment Metrics	20
Appendix E: OSINT Assessment	22
OSINT Findings	22
OSINT Findings	22
Appendix F: Phishing Assessment	34
Exercises	34
Appendix G: Network Details	35
Asset Inventory	35

Appendix H: Tools Used	36
Tool Table	36

1.0 Report Overview

Example: This report documents the results of a penetration test engagement for [Client Name]. It is intended for executive leadership, security teams, and technical staff. The test was conducted as a [black-box/gray-box/white-box] assessment to evaluate the security posture.

1.1 Confidentiality

Example: This document contains sensitive information related to the security of [Client Name]. It must not be distributed, copied, or disclosed without prior written permission. All findings remain the property of [Client Name].

1.2 Legal Disclaimer

Example: The penetration test was performed with full authorization from [Client Name]. While every effort was made to avoid disruption, unforeseen issues may occur. The testing team is not liable for damages resulting from remediation actions based on this report.

1.3 Contact Information

CLIENT ORGANIZATION	
Name	[Client Contact Name]
Role	[Client Role / Title]
Email	[Client Email]

TESTING TEAM	
Name	[Tester Name]
Role	[Senior Consultant]
Email	[Tester Email@cptc.team]

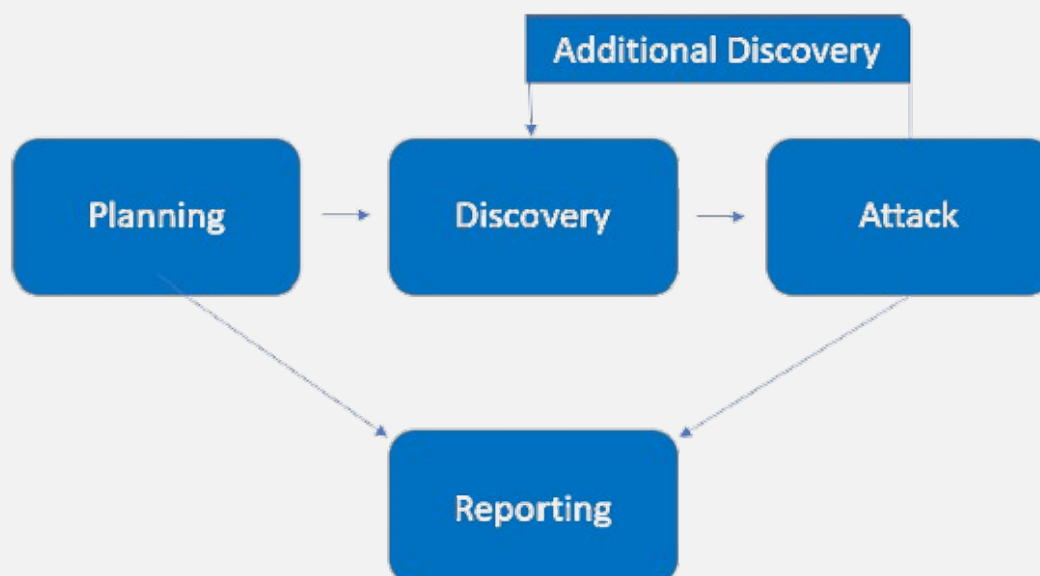
2.0 Executive Summary

2.1 Assessment Overview

Example: From February 22nd, 2021 to March 5th, 2021, Demo Corp engaged TCMS to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network penetration test. All testing performed is based on the NIST SP 800-115 Technical Guide, OWASP Testing Guide (v4), and customized frameworks.

2.1.1 Phases of Penetration Testing

- **Planning** – Customer goals and rules of engagement obtained.
- **Discovery** – Scanning and enumeration to identify vulnerabilities.
- **Attack** – Confirm vulnerabilities via exploitation.
- **Reporting** – Document findings, successes, and failures.



2.2 Scoping and Time Limitations

Briefly describe engagement scope, exclusions, and any time limitations.

2.3 Testing Summary

Example: The team conducted an internal network assessment of Demo Corp to evaluate its overall security posture. The assessment included vulnerability scanning of all provided IPs to determine patching health, common Active Directory attacks such as LLMNR poisoning, SMB relaying, IPv6 man-in-the-middle relaying, and Kerberoasting, as well as an evaluation of other risks including open file shares, default credentials, and sensitive information exposure. The team discovered that LLMNR was enabled, allowing the interception of user hashes, which were subsequently cracked via dictionary attacks, indicating a weak password policy. Using these credentials, the team accessed multiple machines, highlighting overly permissive user accounts. Older operating systems enabled WDigest attacks, exposing cleartext credentials, and reused local account hashes allowed additional machine access through pass-the-hash attacks. Lateral movement eventually led to the compromise of a Domain Administrator account. Additional critical risks included delegation attacks, SMB relay vulnerabilities, unrestricted IPv6 traffic, and unpatched devices with remote code execution vulnerabilities.

2.4 Tester Notes & Recommendations

Example: The findings suggest that Demo Corp is undergoing its first penetration test, with weak password policies and insufficient patch management being primary contributors to network compromise. The team recommends implementing stronger password policies, with a minimum of 15 characters for standard users and 30 for Domain Administrators, exploring password blacklisting, and considering a Privileged Access Management solution. Weak patching and outdated operating systems contributed to the compromise of multiple machines; therefore, Demo Corp should review patching recommendations, address vulnerabilities identified in the Technical Findings section, and improve patch management procedures. On a positive note, several attacks triggered alerts, indicating that the Security Operations team is actively monitoring the network. Overall, the network performed as expected for a first-time assessment, and the team recommends remediating all findings and conducting annual retesting to enhance the internal security posture.

3.0 Assessment Components

3.1 Open-Source Intelligence

Example tailor it more to the company though: OSINT emulates an attacker gathering publicly available information about the organization. Engineers collect data from websites, social media, and other sources to identify potential weaknesses and entry points.

3.2 External Penetration Test

Example tailor it more to the company though: An external penetration test emulates an attacker outside the organization's network. Engineers scan public assets to identify and exploit weaknesses.

3.3 Internal Penetration Test

Example tailor it more to the company though: An internal penetration test emulates an attacker from inside the network. Engineers scan internal hosts and perform internal network attacks.

4.0 Scope

The table below lists all workstations and hosts included in the scope of this assessment, along with their operating systems and IP addresses.

Workstation / Host Inventory	
OS	IP Address
Linux (Kali 2024.1)	10.10.10.11
Windows Server 2019	10.10.5.20
Windows 10	10.10.10.12

The table below summarizes the network subnets included in the scope, along with a brief description of each subnet's purpose.

Network Scope	
Subnet (CIDR)	Description
10.10.10.0/24	Tester workstations and pentest tools
10.10.5.0/24	Internal application servers (AD, DB, app servers)
203.0.113.0/28	Public-facing lab services (web, VPN)
10.10.1.0/24	Management network / admin workstations (out-of-scope)

4.1 Scope Exclusions

List systems excluded from testing.

4.2 Client Allowances

Describe client-provided access, credentials, or permissions.

4.3 Network Topology

Insert network diagrams for the engagement.

5.0 Compliance Summary

5.1 Compliance1

Compliance Info...

5.2 Compliance2

Compliance Info...

6.0 Technical Finding Summary

Unique ID	Finding	Severity	Impact / CVSS Score
VULN-001	Unpatched Web Server	High	7.6.
VULN-002	Weak Password Policy	Medium	5.4
VULN-003	Open SMB Share	High	7.3
VULN-004	Default Credentials on IoT Device	Medium	5.1
VULN-005	Example Vulnerability	High	7.9

7.0 Technical Findings

7.1 Critical Risk Findings

7.1.1 [Finding Name]

Do subsection for each critical finding

[Unique ID]: Service Account has weak password	
Status: <i>Unremediated</i>	
Findings Categorization: Critical	
CVSS v4.0 Score: 9.3	
CVSS Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/V1:L/VA:H/SC:L/SI:L/SA:H/S:P	

Technical Description

Describe vulnerability in depth.

Business Impact Description

How this impacts the business and what effects this has.

Affected Systems

List systems.

Potential Compliance Violations

List compliance violations.

Remediation

Describe how to fix or patch vulnerability.

References

Provide links to websites, advisories, or CVEs.

Steps for Reproduction

Describe reproduction steps and reference relevant compliance frameworks.

7.2 High Risk Findings

7.2.1 [Finding Name]

Do subsection for each high finding

[Unique ID]: Service Account has weak password	
Status: <i>Unremediated</i>	
Findings Categorization: High	
CVSS v4.0 Score: 7.2	
CVSS Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/V1:L/VA:H/SC:L/SI:L/SA:H/S:P	

Technical Description

Describe vulnerability in depth.

Business Impact Description

How this impacts the business and what effects this has.

Affected Systems

List systems.

Potential Compliance Violations

List compliance violations.

Remediation

Describe how to fix or patch vulnerability.

References

Provide links to websites, advisories, or CVEs.

Steps for Reproduction

Describe reproduction steps and reference relevant compliance frameworks.

7.3 Medium Risk Findings

7.3.1 [Finding Name]

Do subsection for each medium finding

[Unique ID]: Service Account has weak password	
Status: <i>Unremediated</i>	
Findings Categorization: Medium	
CVSS v4.0 Score: 5.6	
CVSS Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/V1:L/VA:H/SC:L/SI:L/SA:H/S:P	

Technical Description

Describe vulnerability in depth.

Business Impact Description

How this impacts the business and what effects this has.

Affected Systems

List systems.

Potential Compliance Violations

List compliance violations.

Remediation

Describe how to fix or patch vulnerability.

References

Provide links to websites, advisories, or CVEs.

Steps for Reproduction

Describe reproduction steps and reference relevant compliance frameworks.

7.4 Low Risk Findings

7.4.1 [Finding Name]

Do subsection for each low finding

[Unique ID]: Service Account has weak password	
Status: <i>Unremediated</i>	
Findings Categorization: Low	
CVSS v4.0 Score: 2.4	
CVSS Vector:	
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/V1:L/VA:H/SC:L/SI:L/SA:H/S:P	

Technical Description

Describe vulnerability in depth.

Business Impact Description

How this impacts the business and what effects this has.

Affected Systems

List systems.

Potential Compliance Violations

List compliance violations.

Remediation

Describe how to fix or patch vulnerability.

References

Provide links to websites, advisories, or CVEs.

Steps for Reproduction

Describe reproduction steps and reference relevant compliance frameworks.

7.5 Informational Risk Findings

7.5.1 [Finding Name]

Do subsection for each informational finding

[Unique ID]: Service Account has weak password	
Status: <i>Unremediated</i>	
Findings Categorization: Informational	
CVSS v4.0 Score: N/A	
CVSS Vector: N/A	

Technical Description

Describe vulnerability in depth.

Business Impact Description

How this impacts the business and what effects this has.

Affected Systems

List systems.

Potential Compliance Violations

List compliance violations.

Remediation

Describe how to fix or patch vulnerability.

References

Provide links to websites, advisories, or CVEs.

Steps for Reproduction

Describe reproduction steps and reference relevant compliance frameworks.

Appendix A: Non-Compliance Findings

Example: Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS Requirements	Related Findings
Protect Account Data	
Requirement 1: Password complexity not enforced for some user accounts	7.2.1
Requirement 2: Multi-factor authentication not enabled for administrative accounts	7.2.2
Data Encryption	
Requirement 3: Some sensitive files stored unencrypted on shared drives	7.1.2
Requirement 4: Backups of confidential data not encrypted at rest	
Vulnerability Management	
Requirement 5: Critical patches missing on Windows Server 2019	
Requirement 6: Web application subnet not scanned for vulnerabilities	

Appendix B: Social Engineering

Methodology

Include methodology, tests, and approach.

Results

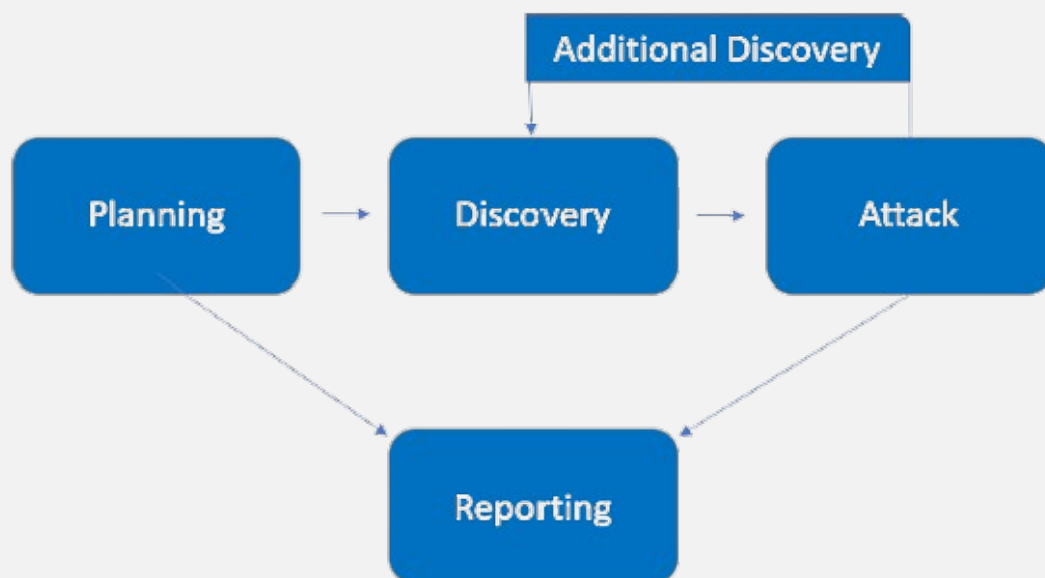
Include test outcomes, success rates, and notable findings.

Appendix C: Methodologies

Testing Frameworks

All testing performed is based on the NIST SP 800-115 Technical Guide, OWASP Testing Guide (v4), and customized frameworks.

Diagrams



Appendix D: Logical Systems

Logical Systems		
Logical System	Abbreviation	Description
Active Directory	AD	Centralized directory service for managing users, groups, and computers in a Windows environment.
Microsoft Exchange	EXCH	Email and calendaring server used for internal communications.
Kali Linux Pentest Workstation	KALI	Linux-based penetration testing workstation with security tools installed.
Windows Server 2019 Lab	WIN-SRV	Server used for lab applications, domain membership, and testing.
Web Application Lab	WEB	Simulated internal and public-facing web services for testing.
Database Lab	DB	Simulated database servers used for testing authentication, queries, and vulnerabilities.

Appendix E: Attack Paths

Visualizations

Illustrate attack chains and lateral movements.

Appendix F: Risk Assessment Metrics

CVSS 4.0 Severity Ratings

Score Range	Severity	Description
0.0	None	No impact, informational only.
0.1 – 3.9	Low	Minimal impact; exploitation unlikely to cause serious harm.
4.0 – 6.9	Medium	Moderate impact; may allow partial compromise or disruption.
7.0 – 8.9	High	Significant impact; exploitation could cause major disruption or breach.
9.0 – 10.0	Critical	Severe impact; straightforward exploitation with catastrophic consequences.

Impact Levels

Level	Name	Description
1	Insignificant	Minimal or no effect; cosmetic issues only.
2	Minor	Limited adverse effect; easily recoverable.
3	Moderate	Noticeable disruption; multi-hour outage or partial data exposure.
4	Major	Significant disruption, financial loss, or reputational impact.
5	Severe (Catastrophic)	Critical impact; long-term damage, legal penalties, or safety concerns.

Likelihood Levels

Level	Name	Description
1	Rare	Very unlikely; requires exceptional circumstances.
2	Unlikely	Possible but improbable; high exploitation complexity.
3	Possible	Could occur; known techniques or PoC exist.
4	Likely	Expected in many cases; active exploitation observed.
5	Almost Certain	Easy and widespread exploitation; automated tools.

Risk Matrix (Impact × Likelihood)

Likelihood ↓ / Impact →	1	2	3	4	5
1	Low	Low	Medium	Medium	High
2	Low	Medium	Medium	High	High
3	Low	Medium	High	High	Critical
4	Medium	High	High	Critical	Critical
5	Medium	High	Critical	Critical	Critical

Appendix G: OSINT Assessment

OSINT Findings

Finding ID	OSINT-I-1
Section Number	G.1
Finding Name	Public Exposure of GitHub Repository via Error Response

Technical Description

During initial reconnaissance, the tester attempted to access the `/robots.txt` file on the target domain `allports.tours`. Instead of receiving a valid `robots.txt` file or a standard HTTP 404 response, the server returned a custom error message that referenced GitHub. This indicates that the web server or its error handling routine is tied to a public GitHub repository, inadvertently revealing the existence of code repositories associated with the organization.

Business Impact Description

The exposure of a GitHub reference in an error response poses significant risks to the organization. Adversaries could leverage this information to identify and access public repositories that may contain sensitive data such as source code, configuration files, or credentials. Beyond direct data leakage, this enables attackers to gather intelligence about the company's technology stack, development practices, and key personnel, supporting targeted phishing or credential stuffing. Additionally, discovery of misconfigured repositories can damage the organization's reputation and erode customer trust.

Source

- Domain: `https://allports.tours/robots.txt`
- Server error response referencing GitHub

Mitigations

1. Standardize error handling with generic templates.
2. Audit GitHub repositories to ensure private repos are not unintentionally public.

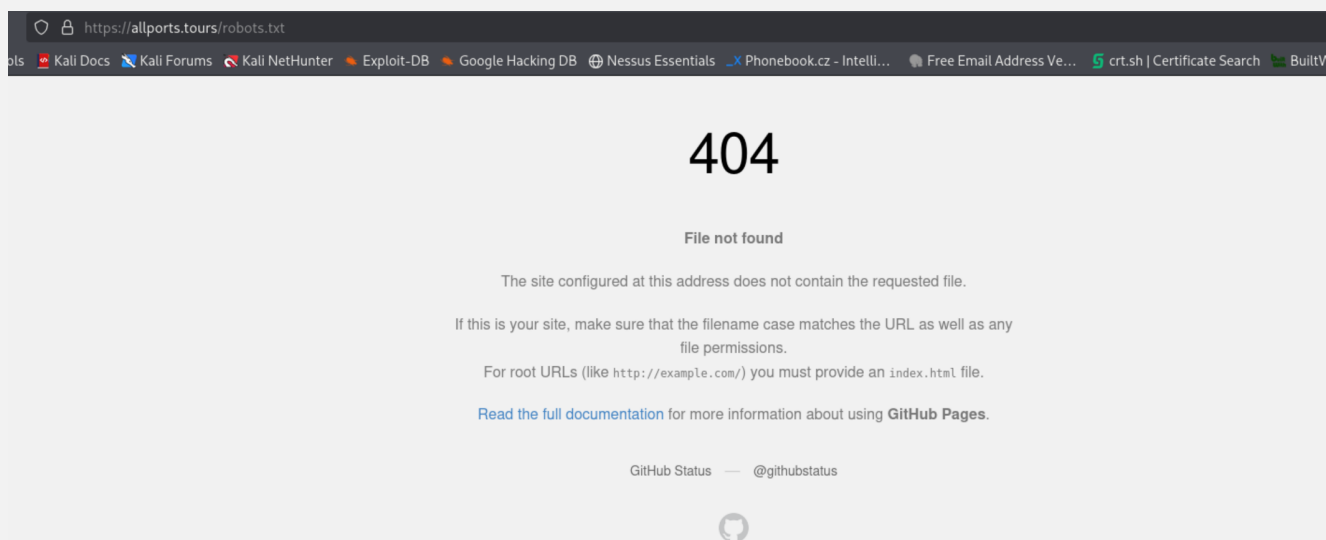
3. Implement monitoring to detect organizational asset references on third-party platforms.
4. Train developers not to embed sensitive details in error messages.

References

N/A

Steps for Reproduction

1. Navigate to `https://allports.tours/robots.txt`.
2. Observe the HTTP response.
3. Note that the response does not return a standard robots.txt but includes a GitHub reference.
4. Use this reference to identify the associated public GitHub repository.



Finding ID	OSINT-I-2
Section Number	G.2
Finding Name	Disclosure of Employee Name in Page Source

Technical Description

While reviewing the source code of the landing page at `allports.tours`, the tester identified the name **Bailey Finn** embedded in the page footer. This disclosure provides

adversaries with specific employee information that can be correlated with platforms like GitHub or LinkedIn for further reconnaissance and social engineering.

Business Impact Description

The disclosure of employee names in publicly accessible web content increases the organization's attack surface by providing adversaries with verified targets for reconnaissance and social engineering. Attackers can correlate names with public profiles, email formats, or repositories to build organizational maps and craft tailored phishing emails or impersonation attempts. Additionally, exposing specific names highlights key staff members as high-value targets for business email compromise (BEC) campaigns.

Source

- Domain: `https://allports.tours`
- HTML page source contained the name **Bailey Finn** in footer

Mitigations

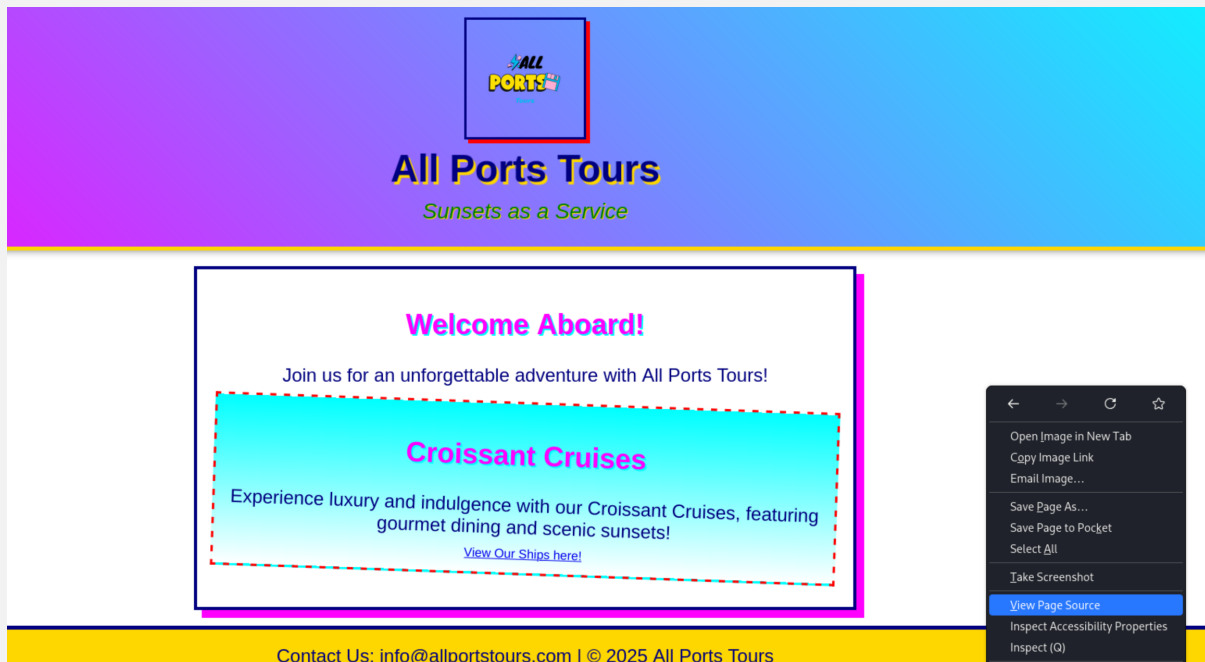
1. Remove unnecessary references to employee names from public-facing pages.
2. Replace acknowledgments with role-based identifiers (e.g., `support@allports.tours`).
3. Train employees to recognize phishing attempts.
4. Conduct OSINT monitoring for unintentional disclosures.

References

N/A

Steps for Reproduction

1. Navigate to `https://allports.tours`.
2. View the page source.



3. Scroll to the footer and observe the name **Bailey Finn**.

```
100     transform: rotate(2deg);
101   }
102   .cruise-option img {
103     width: 100px;
104     border: 2px solid #000080;
105     box-shadow: 3px 3px #FFD700;
106   }
107   footer {
108     background: #FFD700;
109     padding: 10px;
110     font-size: 18px;
111     border-top: 5px solid #000080;
112     color: #000080;
113   }
114   @keyframes pulse {
115     0% { transform: scale(1); }
116     50% { transform: scale(1.1); }
117     100% { transform: scale(1); }
118   }
119   @media (max-width: 600px) {
120     h1 { font-size: 32px; }
121     h2 { font-size: 24px; }
122     p, .slogan { font-size: 18px; }
123     header img, .cruise-option img { width: 100px; }
124   }
125 </style>
126 </head>
127 <body>
128   <header>
129     
130     <h1>All Ports Tours</h1>
131     <p class="slogan">Sunsets as a Service</p>
132   </header>
133   <div class="content">
134     <h2>Welcome Aboard!</h2>
135     <p>Join us for an unforgettable adventure with All Ports Tours!</p>
136     <div class="cruise-option">
137       <h2>Croissant Cruises</h2>
138       <p>Experience luxury and indulgence with our Croissant Cruises, featuring gourmet dining and scenic sunsets!</p>
139       <a href="ships.html">View Our Ships here!</a>
140     </div>
141   </div>
142   <footer>
143     <p>Contact Us: info@allportstours.com | &copy; 2025 All Ports Tours</p>
144   </footer>
145 </body>
146 </html>
147 <!-- ** Written by Bailey Finn ** -->
148
```

Finding ID	OSINT-I-3
Section Number	G.3
Finding Name	Publicly Accessible GitHub Repository Identified

Technical Description

Using GitHub dorking with the query `allports.tours`, the tester identified a publicly accessible repository associated with the organization under the account of **Bailey Finn**. The existence of this repository indicates that organizational artifacts may be hosted publicly, exposing sensitive information.

Business Impact Description

A publicly accessible GitHub repository tied to the organization represents a significant risk. Attackers can obtain sensitive data such as source code, internal documentation, or configuration files. It also reveals insights into development practices, technology stack, and naming conventions. This intelligence accelerates reconnaissance and may facilitate exploitation, code reuse attacks, or social engineering of developers. Publicly exposed repositories can also harm reputation and diminish stakeholder trust.

Source

- GitHub query: <https://github.com/search?q=allports.tours>
- Repository associated with **Bailey Finn**

Mitigations

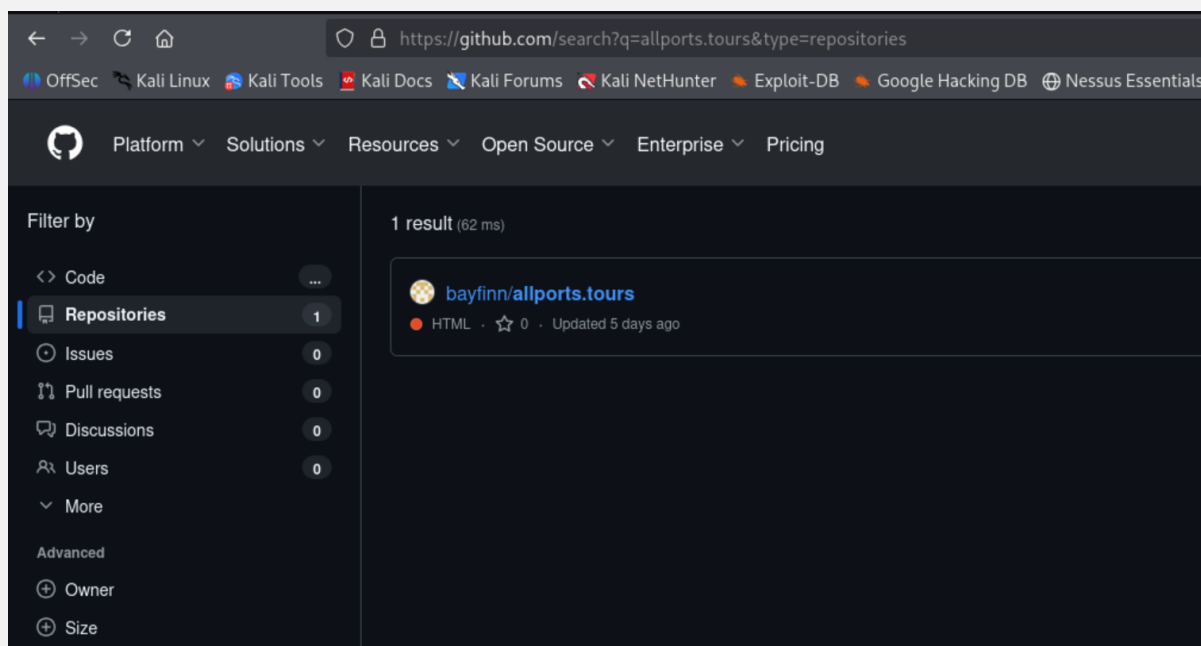
1. Ensure all repositories are private unless intended for public release.
2. Audit and sanitize repositories to remove sensitive data.
3. Enforce GitHub security controls (branch protection, secret scanning).
4. Conduct regular OSINT audits to identify unauthorized repositories.

References

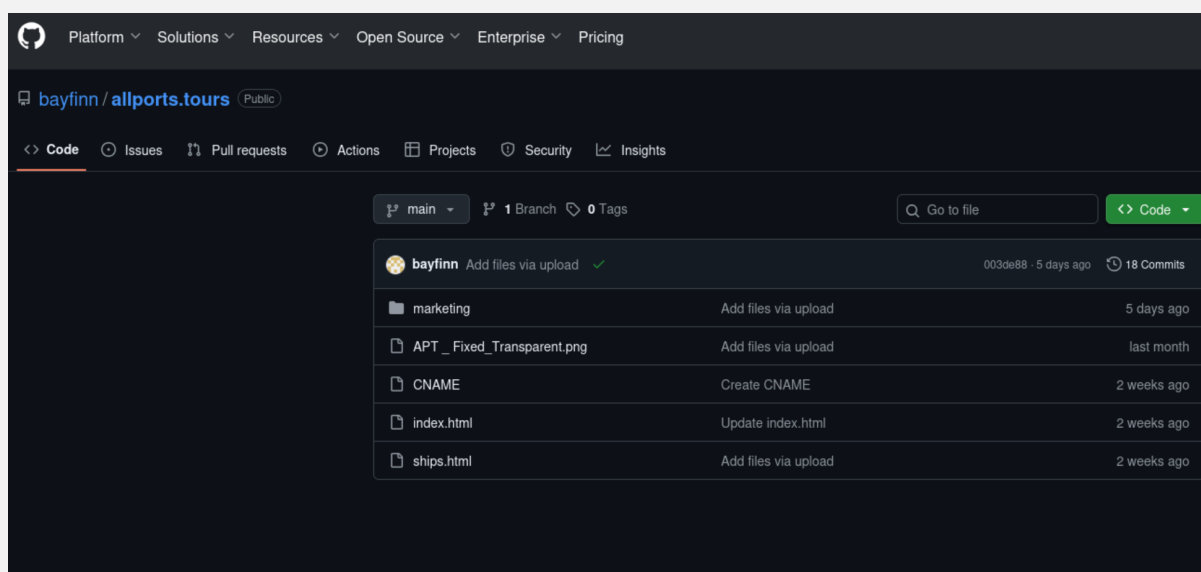
N/A

Steps for Reproduction

1. Navigate to <https://github.com/search?q=allports.tours>.
2. Identify the repository tied to **Bailey Finn**.



3. Confirm it is publicly accessible.



Finding ID	OSINT-I-4
Section Number	G.4
Finding Name	Sensitive Organizational Information in Repository

Technical Description

The tester identified a file named `APT_history.md` in the `/marketing` folder of the public GitHub repository. The file contained leadership details: **David Carter – CEO, Emily**

Carter – COO, and **Bailey Finn – Director of Technical Services**. This information was accessible without authentication.

Business Impact Description

The disclosure of leadership details significantly increases exposure to targeted social engineering and executive-level threats. Attackers can craft convincing phishing or BEC attacks exploiting executive authority. Knowledge of the corporate hierarchy aids in identifying high-value individuals for spear phishing, credential harvesting, or impersonation. Correlation with LinkedIn or WHOIS data further accelerates reconnaissance. Public exposure of such information may also erode trust and damage reputation.

Source

- Public GitHub repository: `allports.tours`
- File: `/marketing/APT_history.md`

Mitigations

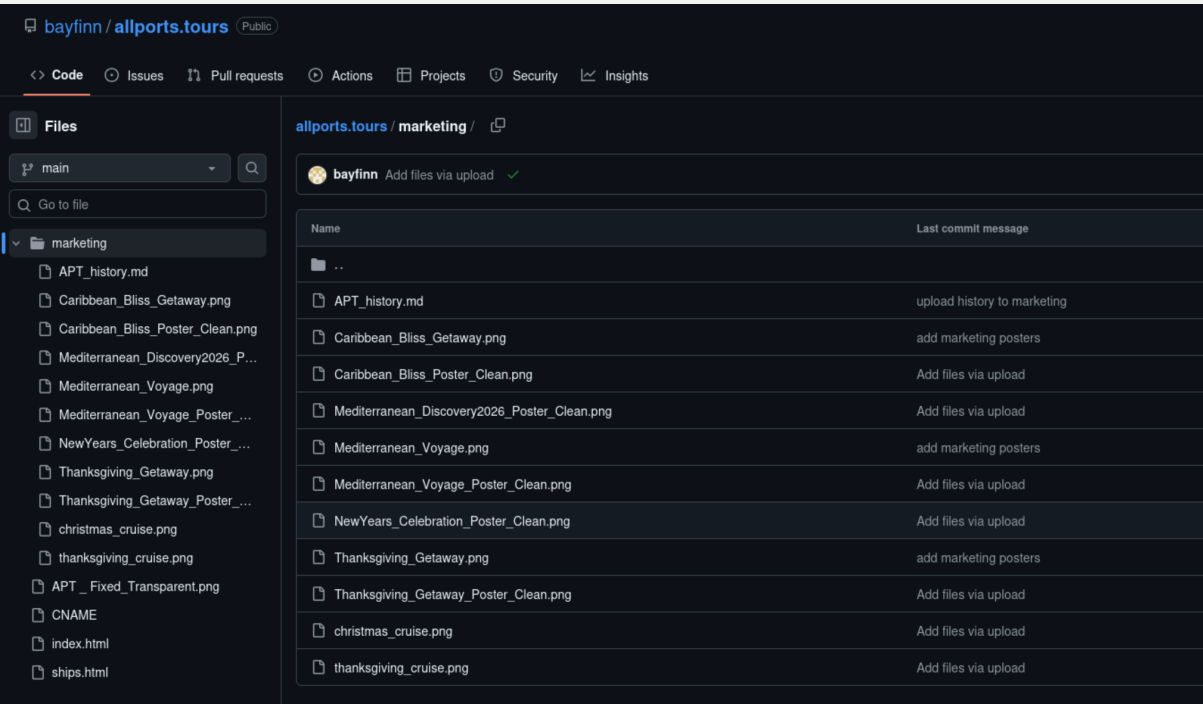
1. Make repositories private or remove sensitive files.
2. Enforce data classification policies for sensitive information.
3. Train employees on risks of public exposure.
4. Monitor external platforms for leaks and request takedowns.

References

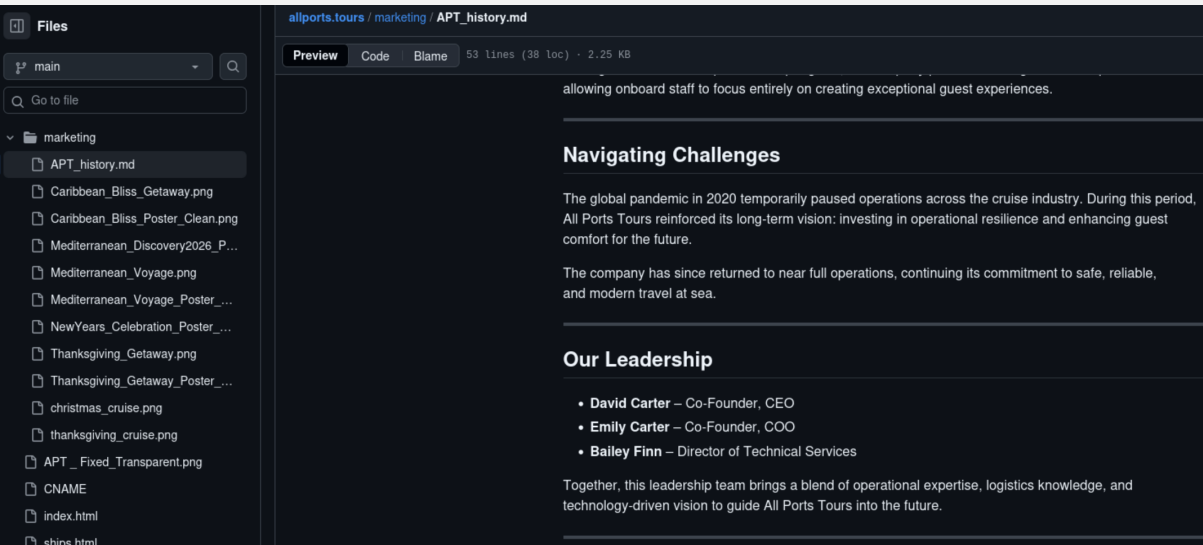
N/A

Steps for Reproduction

1. Navigate to the identified repository.
2. Browse to the `/marketing` folder.



3. Open APT_history.md and observe leadership details.



Finding ID	OSINT-I-5
Section Number	G.5
Finding Name	Employee Email Address Exposed via Git Commit Metadata

Technical Description

Analysis of commit history revealed the internal employee email: Bailey.Finn@allports.tours.

Git metadata automatically attaches contributor email addresses to commits unless masked.

Business Impact Description

Exposure of valid corporate email addresses increases the risk of phishing, spam, and credential-based attacks. The format `FirstName.LastName@allports.tours` allows enumeration of additional employees. This facilitates spear phishing, credential stuffing, and impersonation. Public repositories also risk email scraping for malicious resale, creating long-term threats.

Source

- Public GitHub repository: `allports.tours`
- Git commit metadata (`git log`)

Mitigations

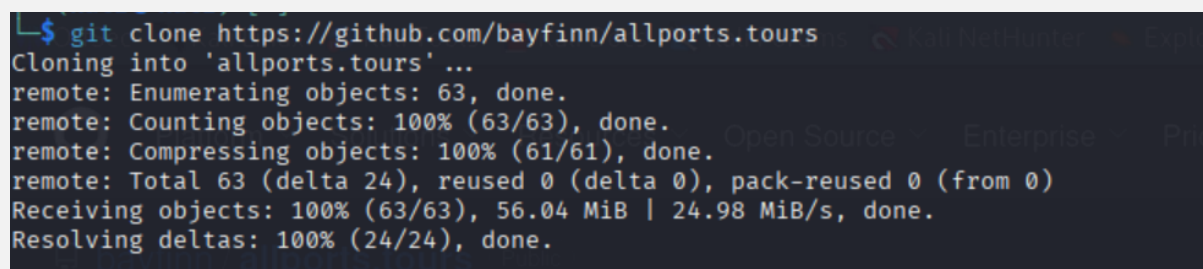
1. Rewrite Git history to remove exposed emails.
2. Enable GitHub's "noreply" feature for commits.
3. Require developers to use obfuscated or role-based commit emails.
4. Monitor inbound traffic for phishing attempts.

References

<https://git-scm.com/docs/pretty-formats>

Steps for Reproduction

1. Clone the public repository.



```
$ git clone https://github.com/bayfinn/allports.tours
Cloning into 'allports.tours' ...
remote: Enumerating objects: 63, done.
remote: Counting objects: 100% (63/63), done.
remote: Compressing objects: 100% (61/61), done.
remote: Total 63 (delta 24), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (63/63), 56.04 MiB | 24.98 MiB/s, done.
Resolving deltas: 100% (24/24), done.
```

2. Run `git log --pretty=full`.
3. Review commits for contributor emails.

4. Confirm Bailey.Finn@allports.tours is exposed.

```
(kali㉿kali)-[~/allports.tours]
$ git log --pretty=full
commit 003de88d17ec7d50dc91e2c5faa3e2fb1610af8e (HEAD -> main, origin/main, origin/HEAD)
Author: bayfinn <bailey.finn@allports.tours>
Commit: GitHub <noreply@github.com>

    Add files via upload

commit 8a7fc255b12066f6cf8cd017d6dc2a5088abbfdc
Author: bayfinn <bailey.finn@allports.tours>
Commit: GitHub <noreply@github.com>

    Add files via upload

commit 8776a889524264a699d48b7bcc0b83f79d3f3efc
Author: bayfinn <bailey.finn@allports.tours>
Commit: GitHub <noreply@github.com>

    Delete marketing/Thanksgiving_Getaway_Poster.png

commit 24165fd9cb764ead3dd312773db806f9b7565322
Author: bayfinn <bailey.finn@allports.tours>
Commit: GitHub <noreply@github.com>

    Delete marketing/NewYears_Celebration_Poster.png

commit 80301ad618daa2b1835a44b4896941d579d1a359
Author: bayfinn <bailey.finn@allports.tours>
Commit: GitHub <noreply@github.com>

    Delete marketing/Mediterranean_Voyage_Poster.png

commit 17be33650e99a1b559c09889d0e8a3cf6343262f
Author: bayfinn <bailey.finn@allports.tours>
Commit: GitHub <noreply@github.com>

    Delete marketing/Mediterranean_Discovery2026_Poster.png

commit 874035618b05248ede0d22e62bdb4abd80750928
Author: bayfinn <bailey.finn@allports.tours>
Commit: GitHub <noreply@github.com>
```

Finding ID	OSINT-I-6
Section Number	G.6
Finding Name	User Attribution Through GitHub Username Pattern

Technical Description

The repository owner's GitHub username was bayfinn, a direct abbreviation of employee **Bailey Finn**. This creates a strong attribution link between the repository and the employee, validating their role in managing public organizational repositories.

Business Impact Description

Identifiable usernames increase attribution risk by linking accounts to employees. Adversaries can correlate usernames with personal data, aiding spear phishing, credential stuffing, or impersonation attempts. Technical staff with identifiable usernames may be targeted as privileged assets, increasing the chance of compromise.

Source

- Public GitHub repository: `allports.tours`
- GitHub username: `bayfinn`
- Correlated identity: **Bailey Finn**

Mitigations

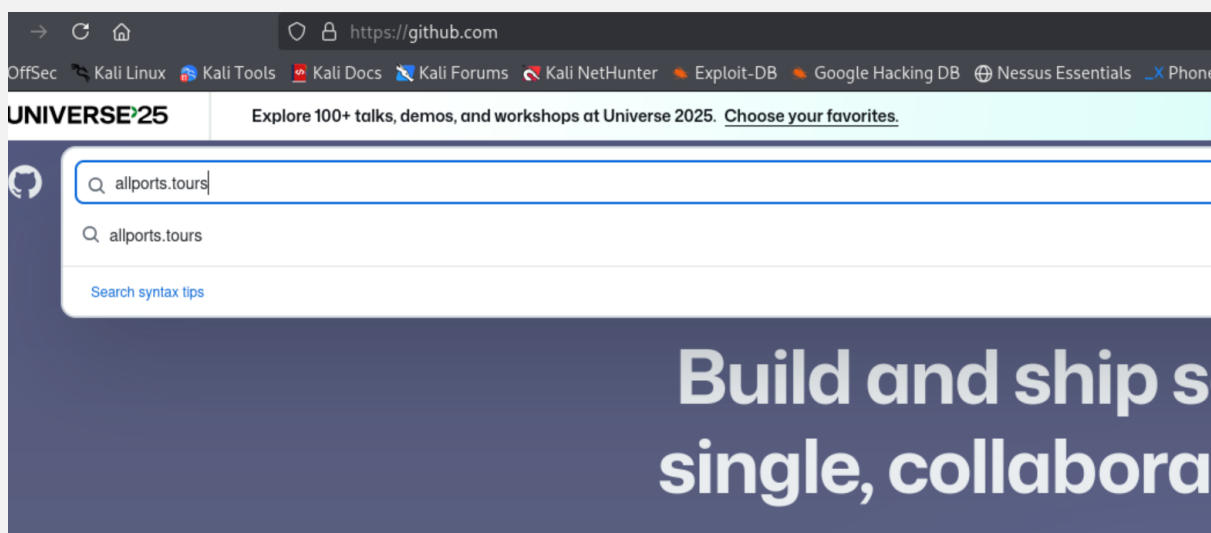
1. Use generic or role-based usernames for corporate accounts.
2. Train staff on risks of identifiable usernames.
3. Limit public exposure of repositories tied to personal accounts.
4. Periodically review usernames tied to organizational assets.

References

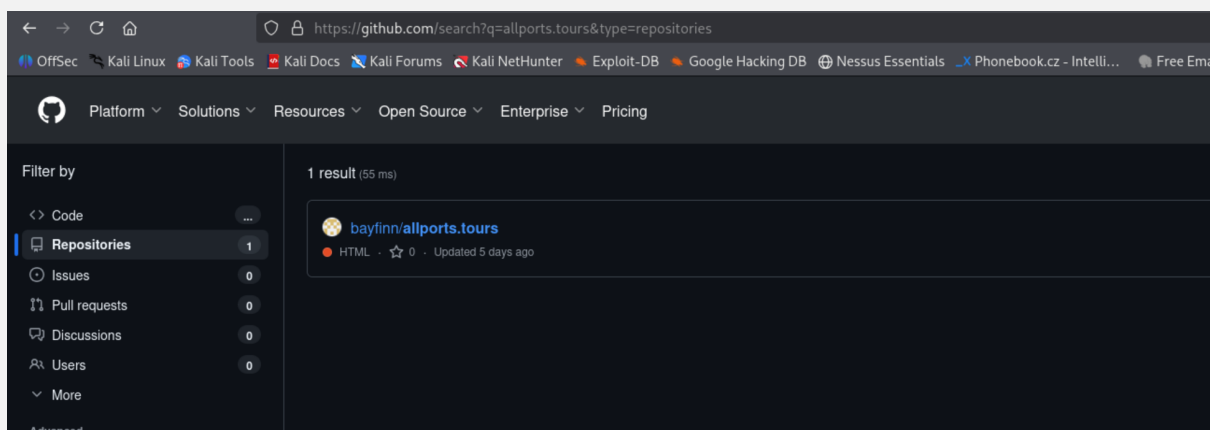
N/A

Steps for Reproduction

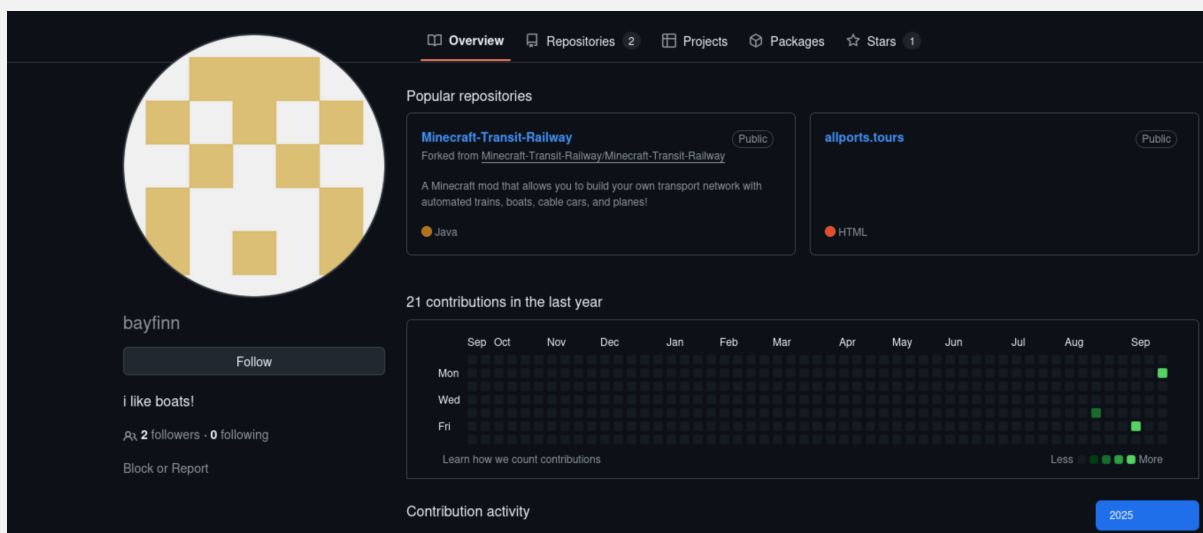
1. Search GitHub with `allports.tours`.



2. Locate repository owner `bayfinn`.



3. Correlate with previously identified employee **Bailey Finn**.



Appendix H: Phishing Assessment

Exercises

Summarize phishing exercises and results.

Appendix I: Network Details

Asset Inventory

IP addresses, FQDNs, open ports, and other relevant information.

Appendix J: Tools Used

Tool Table

Include type (exploitation, post-exploitation, reconnaissance), description, and source.